

Re: Deny access to certain IP address

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-09/0078.html>

From: Karl Levinson, mvp (levinson_k_at_despammed.com)

Date: 09/03/05

Date: Fri, 2 Sep 2005 20:33:11 -0400

As an aside, I find it takes longer to figure out the best solution when a post is posted as "how do I do X" instead of "here is my problem, what do I do?" Sometimes, the thing being asked is not the best solution, or further details are needed.

"Dave Morschhauser" <someone@microsoft.com> wrote in message news:eKS7o49rFHA.2604@TK2MSFTNGP14.phx.gbl...

> *Craig --*

>

> *It sounds like what you are really worried about is viruses and spyware from*

> *an organization you have no control over, but who currently has unlimited*

> *access to your network. I think what you really want is a firewall between*

> *the "guest" company and your own servers and computers. You're right this isn't a permissions problem.*

>

> *An easy way to do this would be to set-up a second broadband router on your*

> *first network by connecting its WAN port into one of the LAN ports on the*

> *original router. Leave the guests on the original network, and hide all*

> *your servers and PCs behind the second router. The guests continue to use*

> *the original default gateway, and the new broadband router gets an address*

> *on its WAN port from the DHCP server in the original router. Your servers*

> *and PC now get their addresses from the DHCP server in the new router.*

You

> *need to make sure that the DHCP servers in each of the routers are serving*

> *addresses using a different subnet so that the new router doesn't get*

> *confused about what machines are supposed to be where.*

>

> *You didn't give us much information on how your network is configured, so*

I

> *am making some assumptions based on 90% of the set-ups that are out there.*

> *Unfortunately, this would not be a reasonable solution if you need to*

expose

> *ports on your servers in order to serve the public internet, for example*

> *your company website or e-mail server.*

>

microsoft.public.security: Re: Deny access to certain IP address

> *Hope this helps.*
> *Dave Morschhauser*
>
>
> *It sounds like*
> *"Craig B" <CraigB@discussions.microsoft.com> wrote in message*
> *news:630F3EDA-8E0E-498F-831B-1343C5C0160A@microsoft.com...*
>> *The reason since you want to know is that we have non domain users*
working
> *in*
>> *our offices that work for another company we have no control over that's*
> *the*
>> *real world reason. Sure i would like to either make them a domain user*
> *and*
>> *control their pc's or just say no they can't get on our network but I*
> *don't*
>> *have that power. They use us just as a dhcp provider then use our*
internet
>> *and in the process spew their spyware all over our network.*
>>
>> *"Karl Levinson, mvp" wrote:*
>>
>>> *You lose accountability if users use shared accounts. That's not a*
>>> *Microsoft thing. I guess there could be some "real world" reasons why*
> *you*
>>> *would need to use shared accounts, like poorly written apps, but it's*
to
> *be*
>>> *avoided.*
>>>
>>> *You can use IPSec rules to block access per IP address. Note that*
with
>>> *Microsoft IPsec it is not really feasible to log and view the traffic.*
> *I*
>>> *agree with the other posters that this is not likely to be as secure*
or
>>> *reliable as blocking per user ID, because all that user needs to do is*
> *log*
>>> *into a different account, or set a static IP address instead of*
getting
> *one*
>>> *from DHCP. Whatever caused your environment to deviate from best*
> *security*
>>> *practices, I hope it's possible to reconsider this.*
>>>
>>> <http://securityadmin.info/faq.asp#ipsec>
>>>
>>>
>>> *"Craig B" <CraigB@discussions.microsoft.com> wrote in message*
>>> *news:FAFF801A-ED8C-43B8-8ACE-5F514AA280C0@microsoft.com...*
>>>> *It's a long story but basically I work in the real world where*

microsoft.public.security: Re: Deny access to certain IP address

> *everything*
> > > *isn't always the perfect MS way. Permissions will not work.*
> > > >
> > > *I will look for other methods*
> > > >
> > > *"Phillip Windell" wrote:*
> > > >
> > > > *That is the wrong approach. You should be controlling access based*
> *on*
> > > *who*
> > > > *the user is,...not what thier IP# happens to be. what do you mean*
> *by*
> > > > *"Permissions won't work at this point"? There is no reason*
> *permissions*
> > > > *shouldn't work.*
> > > > >
> > > > > *--*
> > > > > *Phillip Windell [MCP, MVP, CCNA]*
> > > > > *www.wandtv.com*
> > > > > -----
> > > > > *Understanding the ISA 2004 Access Rule Processing*
> > > > > *http://www.isaserver.org/articles/ISA2004_AccessRules.html*
> > > > > >
> > > > > *Microsoft Internet Security & Acceleration Server: Guidance*
> > > > > *<http://www.microsoft.com/isaserver/techinfo/Guidance/2004.asp>*
> > > > > *<http://www.microsoft.com/isaserver/techinfo/Guidance/2000.asp>*
> > > > > >
> > > > > *Microsoft Internet Security & Acceleration Server: Partners*
> > > > > *<http://www.microsoft.com/isaserver/partners/default.asp>*
> > > > > > -----
> > > > > >
> > > > > >
> > > > > > *"Craig B" <CraigB@discussions.microsoft.com> wrote in message*
> > > > > > *news:E968040C-4DA1-4560-B52A-851AACCAD3B7@microsoft.com...*
> > > > > > *> How would you go about denying access to various 2000/2003*
servers
> *to*
> > > *one*
> > > > > *specific IP address?*
> > > > > >
> > > > > > *I know how to block at my firewall but a internal user is inside*
> *and I*
> > > > > *need*
> > > > > > *to block his access to various servers. Permissions won't work*
at
> > > *this*
> > > > > *point*
> > > > > > *I used DHCP to lock his pc to a certain IP address and now I*
want
> *to*
> > > *block*

microsoft.public.security: Re: Deny access to certain IP address

> > > > > *this ip address access to various servers.*

> > > > >

> > > > > *Thanks*

> > > > >

> > > > >

> > > > >

> > >

> > >

> > >

>

>